PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-185376
(43)Date of publication of application : 16.07.1996

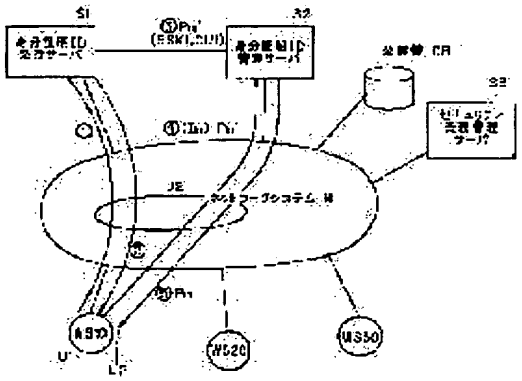
(51)Int.CI. G06F 15/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-327267
(22)Date of filing : 28.12.1994

(71)Applicant : HITACHI LTD
(72)Inventor : SAITO YOKO

(54) MESSAGE TRUST SYSTEM

(57)Abstract:
PURPOSE: To improve the reliability of security work for a highly secret message transmitted/received through a network.
CONSTITUTION: An identification(ID) issuing server S1 and an ID managing server S, issue an ID card IDPU inherent in a user U1 in accordance with the request from the user U1. The user U1 presents a trust condition for a message to a security work managing server S3 by the use of the ID card IDPU1 and the server S3 executes security work such as the storage, publication and cancelation of the message based upon the trust condition. Data communication through a network N protects the secrecy of the ID card IDPU1 and the message by an open key ciphering system. In addition, evidence information indicating that a preparator is the user U1 himself (or herself) and evidence information proving that the ID card IDPU1 is an original are added to a trusted message.



LEGAL STATUS

[Date of request for examination] 10.02.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－185376

(43)公開日　平成８年(1996)７月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ａ	9364－5L		
Ｈ０４Ｌ　9/00				
9/10				
9/12				
			Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全 17 頁）

(21)出願番号　特願平6－327267

(22)出願日　平成６年(1994)12月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　斎藤　洋子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　武　顕次郎

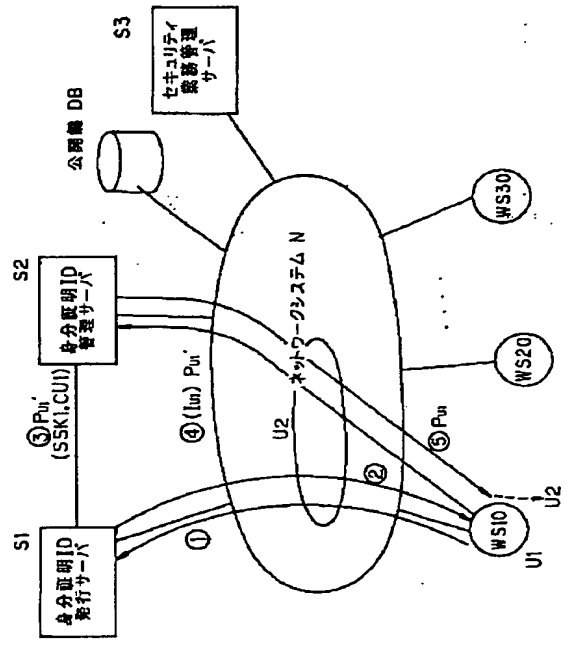
(54)【発明の名称】　メッセージの信託システム

(57)【要約】　（修正有）

【目的】　メッセージの信託システムに関し、ネットワーク経由で送受信される機密度の高いメッセージについてのセキュリティ業務の信頼性を向上させる。

【構成】　身分証明ＩＤ発行サーバS_1および身分証明ＩＤ管理サーバS_2は、ユーザU_1からの要求に応じて当該ユーザU_1固有の身分証明ＩＤＰU_1を発行および交付する。ユーザU_1は、身分証明ＩＤＰU_1を用いてセキュリティ業務管理サーバS_3にメッセージについての信託条件を提示し、これに基づいてセキュリティ業務管理サーバS_3は、メッセージの保管，公開，破棄などのセキュリティ業務を行う。ネットワークＮを介したデータ通信では、公開鍵暗号方式によって身分証明ＩＤＰU_1やメッセージの機密保護を図る。また、信託するメッセージには、作成者がユーザU_1であることを示す証拠情報や、原本であることを証明する証拠情報を付加する。

【図４】



1

【特許請求の範囲】

【請求項１】　ネットワークを介して相互に接続された複数のワークステーション間でメッセージの送受信を行うシステムにおいて、

特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明ＩＤの発行および管理を行う身分証明ＩＤ登録手段と、

前記セキュリティ業務を利用するために前記身分証明ＩＤを用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、

前記身分証明ＩＤを用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段と、を具備する構成としたことを特徴とするメッセージの信託システム。

【請求項２】　各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、

前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備する構成としたことを特徴とする請求項１記載のメッセージの信託システム。

【請求項３】　システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、

前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備する構成としたことを特徴とする請求項２記載のメッセージの信託システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はメッセージの信託システムに係り、特に、ネットワーク経由で機密度の高いメッセージの送受信が行われるメッセージの信託システムに関する。

【０００２】

【従来の技術】従来より、ネットワークを介して接続されているワークステーション（以後、“ＷＳ”と略記する）相互間で行われるメッセージの送受信を保証するための技術として、通信回線上の伝送データやファイル中の記録データを暗号化する技術が知られている。また、特開平５－２６８５９５号公報記載の発明においては、メッセージの内容そのものを保証する方法が提案されており、さらに、特開平２－１８９６３６号公報記載の発明においては、データ送信元のシステム内にネットワーク内のすべての転送経路を示す経路情報と転送データへのアクセスが許されるシステム群を示すデータ属性とを用いることで送信者が任意の転送経路を選択可能とする方法が提案されている。このほか、メッセージを保管する機能については、一般的に電子メールのメールボックス機能やデータベース機能などによって実現されている。

2

【０００３】

【発明が解決しようとする課題】上述したメッセージの送受信に関連する従来技術は、メッセージの保証や転送および保管などの個々の機能に対しては有効であるが、業務内容によっては必ずしも有効に適用できない場合がある。例えば、世間一般に認められた機関（法律事務所など）に対して依頼者が何らかのメッセージ（遺言書など）を登録し、一定の条件のもとで対象者に当該メッセージを開示させる（依頼者が死亡した時点で利害関係人に当該遺言書を公開させるなど）という高度なセキュリティを要するサービス業務をペーパレスで実現しようとする場合、上記従来技術に加えてさらに以下に示すような要件が必要となってしまうという問題点があった。

【０００４】①信託されたメッセージが“文書”として認められること。

・信託すべきメッセージは所定の形式にしたがって作成されており、特に必要な場合にはシステム管理者や関連機関の承認を経ていなければならない。

【０００５】・信託すべきメッセージについて、依頼者本人による原本であって、いかなる改竄もなされていないことが保証されなければならない。

【０００６】②信託されたメッセージが確実に保管管理されること。

・依頼者に登録されたメッセージは、依頼者から指定された信託条件の通りに管理されていなければならない。

・信託されたメッセージの内容は、第三者に盗用されないように確実に秘匿されなければならない。

・信託されたメッセージに対する第三者の不正なアクセスを防止するため、ネットワークを含むシステム内で発生する動作事象を常に監視しなければならない。

【０００７】したがって本発明の目的は、上記の問題点を解決して、ネットワーク経由で送受信される機密度の高いメッセージについてのセキュリティ業務の信頼性を向上させることのできるメッセージの信託システムを提供することにある。

【０００８】

【課題を解決するための手段】

(1) 上記の目的を達成するため、本発明のメッセージの信託システムは、ネットワークを介して相互に接続された複数のワークステーション間でメッセージの送受信を行うシステムにおいて、特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明ＩＤの発行および管理を行う身分証明ＩＤ登録手段と、前記セキュリティ業務を利用するために前記身分証明ＩＤを用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、前記身分証明ＩＤを用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段

と、を具備する構成としたものである。

【０００９】(2) また、(1)において、各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備する構成としたものである。

【００１０】(3) さらに、(2)において、システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備する構成としたものである。

【００１１】

【作用】上記構成に基づく作用を説明する。

【００１２】(1) 本発明のメッセージの信託システムは、ネットワークを介して相互に接続された複数のワークステーション（ＷＳ）間でメッセージの送受信を行うシステムにおいて、特別なセキュリティ業務を利用するユーザの各々について当該ユーザに固有の身分証明ＩＤの発行および管理を行う身分証明ＩＤ登録手段と、前記セキュリティ業務を利用するために前記身分証明ＩＤを用いてネットワーク経由で送受信されるメッセージを第三者から秘匿する信託メッセージ秘匿手段と、前記身分証明ＩＤを用いてユーザから送信されたメッセージについて当該ユーザが指定した信託条件の通りに前記セキュリティ業務を実行するセキュリティ業務管理手段と、を具備している。すなわち、身分証明ＩＤ登録手段は身分証明ＩＤによって特別なセキュリティ業務を利用するユーザの身元を保証し、セキュリティ業務管理手段は身分証明ＩＤによる身元の保証が完了しているユーザに対してのみメッセージの信託サービスなどのセキュリティ業務を提供するので、不正に情報を取得しようとする意図を持つ悪質なユーザを容易に選別および排除することができる。そして、信託メッセージ秘匿手段はネットワーク経由で送受信されるメッセージの内容を暗号化して、当該メッセージに関わるユーザおよびセキュリティ業務管理手段以外の第三者に知られないようにするので、仮に悪質なユーザにメッセージを取得された場合でも、その盗用などによる損失の発生を未然に防止することができる。

【００１３】(2) また、(1)において、各々のメッセージについて当該メッセージの生成および送受信があったことを示す証拠情報を作成する証拠情報作成手段と、前記メッセージのデータ形式を第三者によって改竄不能なデータ形式に変換する改竄防止手段と、をさらに具備している。すなわち、証拠情報作成手段は身分証明ＩＤによってセキュリティ業務を利用するユーザのＷＳから送信されてきたメッセージについて生成および送受信が行われた事実を証明するための証拠情報を作成するので、セキュリティ業務を利用するユーザの間で紛争が発生した場合、保管しておいた証拠情報を調べることによって紛争の原因を客観的に突き止めることができる。そして、改竄防止手段はメッセージの当事者（例えば、メッセージを作成および送信したユーザと、当該ユーザに対してセキュリティ業務を提供するセキュリティ業務管理手段）以外の第三者に改竄されないようにメッセージのデータ形式を変換するので、メッセージの内容についての信頼性を向上させることができる。

【００１４】(3) さらに、(2)において、システム内で発生した事象についての履歴情報を取得する履歴情報取得手段と、前記履歴情報に基づいて前記セキュリティ業務の侵害に関する監査を行うセキュリティ侵害監査手段と、をさらに具備している。すなわち、履歴情報取得手段は稼動中のシステム内で発生した事象を履歴情報として絶えず記録しており、セキュリティ侵害監査手段は記録された履歴情報を常に分析しているので、悪質なユーザによるセキュリティ侵害を迅速に検出して、早期に適切な処置をとることができる。

【００１５】

【実施例】以下、本発明のメッセージの信託システムの一実施例を図面を用いて詳細に説明する。

【００１６】図１は、本発明のメッセージの信託システムの一構成例を示すブロック図である。同図中、ネットワークシステムＮ上には身分証明ＩＤ発行サーバS_1，身分証明ＩＤ管理サーバS_2（S_1およびS_2が請求項中の“身分証明ＩＤ登録手段”に相当する），セキュリティ業務管理サーバS_3（請求項中の“セキュリティ業務管理手段”に相当する）が存在しており、ネットワークを介して接続されたワークステーションWS_{10}，WS_{20}，WS_{30}から特別なセキュリティ業務の利用要求を行う。以後、セキュリティ業務の一例として、WS_{10}からネットワークシステムＮにアクセスするユーザU_1がセキュリティ業務管理サーバS_3によるメッセージの信託サービスを利用する場合について説明を行う。なお、他のセキュリティ業務としては、メッセージの保管サービス，伝達サービスなども考えられる。

【００１７】メッセージの信託サービスを利用する場合、ユーザは身分証明ＩＤ発行サーバS_1に対して、当該サービスを利用するための特別な身分証明ＩＤの発行を事前に要求し、交付された身分証明ＩＤを用いてメッセージの信託を行う。図２は、身分証明ＩＤの発行要求に伴って図１のシステムで行われるデータ通信について概略的に示す図である。同図中、処理①はユーザU_1が身分証明ＩＤであるPU_1の発行を要求する処理であり、処理②は処理①に応じて身分証明ＩＤ発行サーバS_1からユーザU_1に対して仮の引替え証PU_1'（後日、発行された正式な身分証明ＩＤの交付を受けるための情報）を発行する処理である。処理①において、ユーザU_1は自己を特定する識別情報I_{U1}（通常のユーザＩＤやパスワードなど）を指定して身分証明ＩＤ発行サーバS_1にPU_1の発行

要求を行う。身分証明ＩＤ発行サーバS_1はこの発行要求を確認した後、処理②でユーザU_1に対する仮の引替え証PU_1'の発行処理を行う。仮の引替え証PU_1'は正式な身分証明ＩＤの交付を受ける際に必須の情報なので、ユーザU_1はこれを大切に保管管理する。また、識別情報I_{U1}の内容についても他人に知られないように管理しておく。

【００１８】ところで、セキュリティ業務に関わるシステムとして考慮すべき点は、処理①および②に伴って行われるデータ通信の内容について、セキュリティ業務を侵害して不正に情報を取得しようとする意図を持つ悪質なユーザに知られないようにすることであり、このためにはデータ通信される内容を必ず暗号化しておくことが有効である。例えば、ネットワークシステムＮ内に公知の公開鍵暗号方式（請求項中の“信託メッセージ秘匿手段”および“改竄防止手段”に相当する）を採用し、すべてのユーザU_i，身分証明ＩＤ発行サーバS_1，身分証明ＩＤ管理サーバS_2，セキュリティ業務管理サーバS_3の各々に対して公開鍵および秘密鍵を割当てる。そして、すべてのユーザU_iの公開鍵PK_{Ui}，身分証明ＩＤ発行サーバS_1の公開鍵PK_{S1}，身分証明ＩＤ管理サーバS_2の公開鍵PK_{S2}，セキュリティ業務管理サーバS_3の公開鍵PK_{S3}については、公開鍵データベースを用いて公開し、秘密鍵SK_{Ui}については各々のユーザU_iが別のユーザに知られないように保管管理しておく。そして、データ通信の際に自己の秘密鍵と相手の公開鍵を用いて通信内容を暗号化することにより、悪質なユーザを容易に選別および排除するとともに、仮に悪質なユーザに情報を取得されてもその盗用などによる損失の発生を未然に防止することができる。

【００１９】図３は、図２のデータ通信における機密保護のための処理の流れを示すフローチャートであり、ユーザU_1が自己の秘密鍵SK_{U1}と身分証明ＩＤ発行サーバS_1の公開鍵PK_{S1}を用いて処理①に伴うデータ通信を暗号化する場合の一例を示す。図３において、ユーザU_1は身分証明ＩＤ発行サーバS_1に伝えるべき情報I_{U1}を秘密鍵SK_{U1}で暗号化した後、さらに公開鍵PK_{S1}で暗号化して、暗号化メッセージＭ（$M=ENC_{PKS1}(ENC_{SKU1}(I_{U1}))$）を作成する（ステップ３０１）。そして、この暗号化メッセージＭをネットワークＮを介して身分証明ＩＤ発行サーバS_1に送信する（ステップ３０２）。身分証明ＩＤ発行サーバS_1は、ネットワークＮを介して受信した暗号化メッセージＭを自己の秘密鍵SK_{S1}で解読した後、さらにユーザU_1の公開鍵PK_{U1}で解読して、元の情報I_{U1}（$I_{U1}=DEC_{PKU1}(DEC_{SKS1}(M))$）を得る（ステップ３０３）。ここで、$ENC_{SKU1}(I_{U1})$の内容を復元することができるのは秘密鍵$SK_{S1}$を管理している身分証明ＩＤ発行サーバ$S_1$のみであり、さらに公開鍵$PK_{U1}$で復号化して得た元の情報$I_{U1}$の内容を調べることによって処理①（ステップ３０２）で送信されてきたメッセージがユーザU_1からのものであることを確認できる（ステップ３０４）。

【００２０】同様に処理②についても、身分証明ＩＤ発行サーバS_1はユーザU_1に伝えるべき情報PU_1'，SSK_1，CU_1を自己の秘密鍵SK_{S1}で暗号化した後、さらにユーザU_1の公開鍵PK_{U1}で暗号化して、暗号化メッセージＭ（$M=ENC_{PKU1}(ENC_{SKS1}(PU_1', SSK_1, CU_1))$）を作成する（ステップ３０５）。そして、ネットワークＮを介してこの暗号化メッセージＭをユーザU_1に送信する（ステップ３０６）。ユーザU_1は、ネットワークＮを介して受信した暗号化メッセージＭを自己の秘密鍵SK_{U1}で解読した後、さらに身分証明ＩＤ発行サーバS_1の公開鍵PK_{S1}で解読して、元の情報PU_1'，SSK_1，CU_1を得る（ステップ３０７）。ここで、$ENC_{SKS1}(PU_1', SSK_1, CU_1)$の内容を復元することができるのは秘密鍵$SK_{U1}$を管理しているユーザ$U_1$のみであり、さらに公開鍵$PK_{S1}$で復号化して得た元の情報$PU_1$'，$SSK_1$，$CU_1$の内容を調べることによって処理②（ステップ３０６）で送信されてきたメッセージが身分証明ＩＤ発行サーバS_1からのものであることを確認した後、これらの情報を保管する（ステップ３０８）。

【００２１】なお、処理②において、以降の通信で用いるセション鍵SSK_1や、身分証明ＩＤ管理サーバS_2に対して身分証明ＩＤPU_1の取得要求を行う際のアクセス条件CU_1を付加しておくことにより、身分証明ＩＤの発行業務をより確実に行うことができる。例えば、アクセス条件CU_1によって、指定された期間内に指定されたアクセス経路で身分証明ＩＤ管理サーバS_2に取得要求を行わせるようにすれば、悪質なユーザの介入をより確実に排除しやすくなる。また、処理①および②でやり取りされる情報の内容，情報の保護のレベル，ユーザの資格審査の具体的な方法などについては、セキュリティ業務の管理に必要とされる機密度に応じて任意に決定される。

【００２２】ところで、身分証明ＩＤ発行サーバS_1はユーザから身分証明ＩＤの発行要求を受付けるが、実際に身分証明ＩＤを準備してユーザへの交付を行うのは身分証明ＩＤ管理サーバS_2である。これは、身分証明ＩＤの受付から発行までにある程度の時間がかかることが予想されることから、身分証明ＩＤ発行サーバS_1への発行要求が集中した場合のトラフィック量を考慮したことによる。また、ユーザU_1が身分証明ＩＤ管理サーバS_2に仮の引替え証PU_1'を提示して身分証明ＩＤの交付を要求することで、ユーザU_1の身元を２度にわたって確認できる。すなわち、身分証明ＩＤ管理サーバS_2は、仮の引替え証PU_1'を提示して身分証明ＩＤの交付を要求してきたユーザと先に身分証明ＩＤ発行サーバS_1に対して身分証明ＩＤの発行要求を行ったユーザU_1とが同一のユーザであるか否かを確認するとともに、当該ユーザがアクセス条件CU_1にしたがって身分証明ＩＤの交付を要求してきたか否かを確認し、いずれかを満たさないユーザから

の身分証明ＩＤの交付要求については拒否するようにする。

【００２３】図４は、身分証明ＩＤの登録および発行処理に伴って図１のシステムで行われるデータ通信について概略的に示す図である。同図中、処理③は身分証明ＩＤ発行サーバS_1が身分証明ＩＤ管理サーバS_2に対してユーザU_1の身分証明ＩＤ発行要求を登録する処理、処理④はユーザU_1が身分証明ＩＤ管理サーバS_2に対して身分証明ＩＤの交付を要求する処理、処理⑤は身分証明ＩＤ管理サーバS_2がユーザU_1に対して身分証明ＩＤPU_1を交付する処理である。ここで、処理③においては、図２を用いて説明した処理②で身分証明ＩＤ発行サーバS_1がユーザU_1に対して発行した仮の引替え証PU_1'の情報を身分証明ＩＤ管理サーバS_2に引き渡す。セション鍵SSK_1やアクセス条件CU_1が指定されていれば、これらも身分証明ＩＤ管理サーバS_2に引き渡す。なお、身分証明ＩＤ発行サーバS_1と身分証明ＩＤ管理サーバS_2との間では取扱に機密性を要する情報の交換が行われるので、この両者を繋ぐ通信路については十分に保護しておく。例えば、特殊な保護チャネルを使用する、S_1およびS_2に対するアクセス管理を厳格に行う、S_1およびS_2専用の暗号鍵で暗号化してデータ通信を行う、などによって通信路の保護を図る。

【００２４】処理④において、ユーザU_1は身分証明ＩＤ管理サーバS_2に対して自己の識別情報I_{U1}（処理①で提示した通常のユーザＩＤやパスワードなど）と仮の引替え証PU_1'の情報を提示する。処理⑤において、身分証明ＩＤ管理サーバS_2はユーザU_1から提示された情報を確認し、問題がなければ身分証明ＩＤPU_1を交付する。ここで問題となるのは、身分証明ＩＤPU_1が悪質な第三者の手に渡ってしまった場合である（例えば、正規のユーザU_1に対して交付された身分証明ＩＤPU_1の内容を悪質なユーザU_2が盗み見るというケースなど）。一般的にユーザU_1には自己の身分証明ＩＤPU_1をきちんと管理する義務があるので、ユーザU_1が日常的に使用しているWS_{10}から身分証明ＩＤPU_1が盗まれてしまったときにはユーザU_1側に責任がある。しかしながら、ネットワークＮにおけるデータ通信の過程で身分証明ＩＤPU_1が盗まれてしまったときにはセキュリティ業務を提供する側の責任となるので、ユーザU_1と身分証明ＩＤ管理サーバS_2との間のデータ通信の保護を図ることが必要不可欠である。

【００２５】図５は、図４のデータ通信における機密保護のための処理の流れを示すフローチャートである。同図中、ユーザU_1は身分証明ＩＤ管理サーバS_2に伝えるべき情報（識別情報I_{U1}および仮の引替え証PU_1'など）を秘密鍵SK_{U1}で暗号化した後、さらに公開鍵PK_{S2}で暗号化して、暗号化メッセージＭ（$M=ENC_{PKS2}(ENC_{SKU1}(I_{U1}, PU_1'))$）を作成する（ステップ５０１）。そして、この暗号化メッセージＭをネットワークＮを介して身分証明ＩＤ管理サーバS_2に送信する（ステップ５０２）。なお、セション鍵SSK_1が指定されている場合、暗号化メッセージＭをさらにセション鍵SSK_1で暗号化してから送信すれば、ステップ５０２におけるユーザU_1と身分証明ＩＤ管理サーバS_2との間のデータ通信の機密性向上を図ることができる。身分証明ＩＤ管理サーバS_2は、ネットワークＮを介して受信した暗号化メッセージＭを自己の秘密鍵SK_{S2}で解読した後、さらにユーザU_1の公開鍵PK_{U1}で解読して、元の情報Ｉ（$I=DEC_{PKU1}(DEC_{SKS2}(M))$）を得る（ステップ５０３）。ここで、暗号化メッセージＭから元の情報を復元できるのは秘密鍵SK_{S2}を管理している身分証明ＩＤ管理サーバS_2のみであり、さらに公開鍵PK_{U1}で復号化して得た元の情報Ｉの内容を調べることによって処理④（ステップ５０２）で送信されてきたメッセージがユーザU_1からのものであることを確認できる。続いて、ユーザU_1からのアクセスが指定されたアクセス条件CU_1を満たしているか否かを判定し、満たしていない場合には処理④を拒否する（ステップ５０４）。

【００２６】ユーザU_1からのアクセスがアクセス条件CU_1を満たしている場合、身分証明ＩＤ管理サーバS_2はユーザU_1に応答すべき情報（身分証明ＩＤPU_1，以降のデータ通信で用いる新たなセション鍵SSK_iなど）を自己の秘密鍵SK_{S2}で暗号化した後、さらにユーザU_1の公開鍵PK_{U1}で暗号化して、暗号化メッセージＭ（$M=ENC_{PKU1}(ENC_{SKS2}(PU_1, SSK_i))$）を作成し、ネットワークＮを介してこの暗号化メッセージＭをユーザU_1に送信する（ステップ５０５）。なお、セション鍵SSK_1が指定されている場合、暗号化メッセージＭをさらにセション鍵SSK_1で暗号化してから送信すれば、ステップ５０５における身分証明ＩＤ管理サーバS_2とユーザU_1との間のデータ通信の機密性向上を図ることができる。ユーザU_1は、ネットワークＮを介して受信した暗号化メッセージＭを自己の秘密鍵SK_{U1}で解読した後、さらに身分証明ＩＤ管理サーバS_2の公開鍵PK_{S2}で解読して、元の情報PU_1，SSK_iを得る（ステップ５０６）。ここで、暗号化メッセージＭから元の情報を復元することができるのは秘密鍵SK_{U1}を管理しているユーザU_1のみであり、さらに公開鍵PK_{S2}で復号化して得た元の情報の内容を調べることによって処理⑤（ステップ５０５）で送信されてきたメッセージが身分証明ＩＤ管理サーバS_2からのものであることを確認した後、これらの情報を保管する（ステップ５０７）。

【００２７】一旦、固有の身分証明ＩＤPU_1が発行されると、ユーザU_1はこの身分証明ＩＤPU_1を用いてセキュリティ業務管理サーバS_3にメッセージの信託を依頼することができる。図６は、メッセージの信託処理に伴って図１のシステムで行われるデータ通信について概略的に示す図である。同図中、ユーザU_1はどのようなメッセージをどのように信託するかを表す信託条件CU_2を、身分証明ＩＤPU_1を用いてセキュリティ業務管理サーバS_3に

伝える（処理⑦）。そして、信託条件CU_2について合意が得られた場合、セキュリティ業務管理サーバS_3はユーザU_1に対して回答／指示を返す。このとき、後述する証拠情報の作成のために処理⑤で与えられたセション鍵SSK_2を利用する。一方、セキュリティ業務管理サーバS_3は、事前に身分証明ＩＤ管理サーバS_2からユーザU_1に関する情報を受け取っている（処理⑥）ので、悪質なユーザU_2がユーザU_1であると偽ってメッセージの信託を依頼してきても、これを拒否することができる。なお、身分証明ＩＤ管理サーバS_2とセキュリティ業務管理サーバS_3との間では取扱に機密性を要する情報の交換が行われるので、この両者を繋ぐ通信路については十分に保護しておく。例えば、特殊な保護チャネルを使用する、S_2およびS_3に対するアクセス管理を厳格に行う、S_2およびS_3専用の暗号鍵で暗号化してデータ通信を行う、などによって通信路の保護を図る。

【００２８】図７は、メッセージの信託に際して指定される信託条件CU_2の一例を示す図であり、ユーザU_1は自己のメッセージM_1を公開指定日時T_1が到来したときユーザU_3に対して公開する、という条件であるものとする。また、ユーザU_1はセキュリティ業務管理サーバS_3に信託するメッセージM_1の保護手段（どのような機密性，完全性，アクセス制御，否認不可及び監査機能を提供するか）についても信託条件CU_2で規定する。例えば図７において、機密性レベル＝２，完全性レベル＝１と指定されているので、メッセージM_1のデータ全体を暗号化するとともに改竄検出のためのコードを付加する。また、破棄指定日時T_3が指定されているので、時刻T_3を過ぎたときにメッセージM_1は破棄される。

【００２９】図８は、図６のデータ通信における機密保護のための処理の流れを示すフローチャート（その１）である。同図中、ユーザU_1は自己の秘密鍵SK_{U1}，セキュリティ業務管理サーバS_3の公開鍵PK_{S3}，指定されていればセション鍵SSK_2を用いて、信託するメッセージM_1を暗号化する。原則的に、これらの暗号鍵を用いて暗号化してあれば、メッセージの内容を悪質なユーザU_2に盗み見られる可能性は少ないと期待されるが、“文書”としての効力をより確実なものとするには、メッセージM_1の作成者がユーザU_1であることを保証する証拠情報E_1と送信するメッセージM_1が原本であることを保証する証拠情報E_2とをメッセージM_1に付加する。この証拠情報E_1およびE_2の作成については、セキュリティ業務管理サーバS_3に作成させても、信頼できる第三者機関に作成処理を依頼してもよい（請求項中の“証拠情報作成手段”に相当する）。図８では、信託するメッセージM_1および作成日時情報T_0をユーザU_1の秘密鍵SK_{U1}で暗号化したものを証拠情報E_1とする。さらに、原本性を保証する目的でセキュリティ業務管理サーバS_3から与えられたセション鍵SSK_3を用いて、証拠情報E_1を付加したメッセージM_1を変換したものを証拠情報E_2とする。そして、メッセージM_1に証拠情報E_1およびE_2を付加したものを自己の秘密鍵SK_{U1}，セキュリティ業務管理サーバS_3の公開鍵PK_{S3}，指定されていればセション鍵SSK_2を用いて暗号化することでメッセージM_2を作成し（ステップ８０１）、このメッセージM_2を実際にネットワークＮを介してセキュリティ業務管理サーバS_3に送信する（ステップ８０２）。セキュリティ業務管理サーバS_3は、ネットワークＮを介してメッセージM_2を受信すると、セション鍵SSK_2，ユーザU_1の公開鍵PK_{U1}，自己の秘密鍵SK_{S3}を用いてメッセージM_2から元の情報Ｉ（メッセージM_1，証拠情報E_1およびE_2）を復元して、これらの情報を信託条件CU_2にしたがって管理されるメッセージＤＢ（図示なし）内に安全に保管する。メッセージＤＢに保管されたメッセージおよび証拠情報は図９のフローチャートにしたがって管理されており、信託条件CU_2の条件が満たされてメッセージ公開処理が行われない限り、どんなユーザに対しても内容が公開されることはない。

【００３０】図１０は、図６のデータ通信で作成された証拠情報を確認する処理の流れを示すフローチャートである。以下、受信したメッセージM_2からセキュリティ業務管理サーバS_3が復元した元の情報の各々について、証拠情報をE_1’およびE_2’，メッセージをM_1’，作成日時情報をT_0’としてユーザU_1から送信されたものと区別して表し、図１０にしたがって説明を行う。

【００３１】図１０において、セキュリティ業務管理サーバS_3は、メッセージM_2から復元した証拠情報E_1’をユーザU_1の公開鍵PK_{U1}で復号化する（ステップ１００１）。そして、得られた情報ＩのうちのメッセージM_1”とメッセージM_2から復元したメッセージM_1’とを比較し、等しいか否かを調べる（ステップ１００２）。このとき、必要があれば作成日時情報T_0’についても確認する。メッセージM_1”およびM_1’が等しい場合、メッセージM_1’がユーザU_1に作成されたものであることが確認されるので、次に、メッセージM_2から復元したメッセージM_1’および証拠情報E_1’に対してセション鍵SSK_3を入力パラメタとしてハッシュ関数を施し、証拠情報E_2”を作成する（ステップ１００３）。なお、ユーザU_1およびセキュリティ業務管理サーバS_3は、同一のハッシュ関数を極秘に共有しているものとする。この後、メッセージM_2から復元した証拠情報E_2’と証拠情報E_2”とが等しいか否かを調べる（ステップ１００４）。証拠情報E_2’およびE_2”が等しい場合、メッセージM_1’は原本であって途中で改竄されていないことが確認される。以上のようにしてネットワークＮを介して受信したメッセージM_2から復元した情報Ｉの正当性が確認された後（図８中のステップ８０４）、セキュリティ業務管理サーバS_3はメッセージM_1’と証拠情報E_1’およびE_2’をメッセージＤＢに保管する。

【００３２】ユーザU_1が指定した信託条件CU_2の条件が満たされる（公開指定日時T_1が到来する）と、セキュリ

ティ業務管理サーバS_3は、信託条件CU_2に基づき、公開対象のユーザU_3にメッセージM_1'（＝M_1）を公開する。このとき、セキュリティ業務管理サーバS_3は、メッセージＤＢ中に保管しておいたメッセージM_2の取り出し，その内容確認，メッセージM_1'の作成者がユーザU_1であることおよび原本であることの確認などを、図１０に示したのと同様の手順で行う。

【００３３】図１１は、図６のデータ通信における機密保護のための処理の流れを示すフローチャート（その２）であり、図１０の確認処理に引き続いてセキュリティ業務管理サーバS_3がメッセージM_1を公開対象のユーザU_3に送信する処理（図６中の処理⑨に相当する）を示す。このデータ通信に際しても、セキュリティ業務管理サーバS_3の秘密鍵SK_{S3}およびユーザU_3の公開鍵PK_{U3}によってメッセージM_1を暗号化して送信する。ユーザU_3本人であれば、受信した暗号化メッセージを自己の秘密鍵SK_{U3}で解読可能であり、セキュリティ業務管理サーバS_3の公開鍵PK_{S3}で解読することによって受信した暗号化メッセージが間違いなくS_3に保証されたものであることを確認できる。また、図１１においてM_3はセキュリティ業務管理サーバS_3が添付して送信するメッセージである。

【００３４】次に、メッセージM_1を信託したユーザU_1とメッセージM_1を公開されたユーザU_3との間で信託メッセージの送受信に関する紛争が発生したときにセキュリティ業務管理サーバS_3が果たすべき役割について述べる。メッセージM_1を信託する側のユーザU_1とセキュリティ業務管理サーバS_3との間では、前述した証拠情報E_1およびE_2を作成することによって処理過程にかなりの機密度が保証される。しかしながら、メッセージM_1を受け取る側のユーザU_3については、以下に示すような原因からトラブルが発生する可能性がある。

(A) ユーザU_3がメッセージM_1を受け取った旨の応答を行わない。

(B) ユーザU_3がM_1と異なるメッセージを受け取ったと主張する。

(C) ユーザU_3の管理不全により、悪質なユーザU_2にメッセージM_1を盗用される。

【００３５】上記(A) のケースについては、信託条件CU_2の中で信託メッセージの受け渡し方を規定しておくことにより、トラブルの解決および発生防止を図ることができる。例えば、信託メッセージの送信リトライ回数を指定したり、義務付けた応答をユーザU_3が返してこない場合には受信したものと解釈する、などである。この他、信頼できる配送サーバを通信経路の途中に設けて、データ通信が行われたことを示すE_3を作成しておくことなども有効である。

【００３６】上記(B) のケースについては、前述した証拠情報E_1，E_2，E_3をユーザU_3に提示することで、トラブルの解決および発生防止を図ることができる。すなわち、証拠情報E_1によってメッセージM_1が間違いなくユーザU_1に作成されたことを、証拠情報E_2によってメッセージM_1の原本性（修正されずに保管されていたこと）を、証拠情報E_3によって信託されたときの状態でセキュリティ業務管理サーバS_3からユーザU_3にメッセージM_1が渡されたことを、それぞれ証明できる。

【００３７】上記(C) のケースについては、ユーザU_3の責任によることが明らかであるが、セキュリティ業務管理サーバS_3は、ユーザU_3に対してメッセージM_1を送信する以前にメッセージM_1の内容が漏洩したのではないことをセキュリティ監査機能によって証明して、トラブルの解決および発生防止を図ることができる。図１２は、セキュリティ監査機能を概略的に示すフローチャートであり、セキュリティ関連の事象についてのメッセージの収集手段，メッセージ分析手段，メッセージ記録手段，メッセージ選択手段，セキュリティレポート作成手段などを有する（請求項中の“履歴情報取得手段”に相当する）。そして、得られたセキュリティレポートの情報を分析し、ネットワークシステム全体の弱点を診断する手段（請求項中の“セキュリティ侵害監査手段”に相当する）も提供されているので、これを利用して上記の証明を行うことは可能である。なお、セキュリティ監査機能の詳細については、本出願人による特願平６－４７１９４号出願に添付した明細書「セキュリティ管理装置」に記載があるので、説明を省略する。

【００３８】

【発明の効果】以上詳しく説明したように、本発明のメッセージの信託システムによれば、身分証明ＩＤ登録手段は身分証明ＩＤによって特別なセキュリティ業務を利用するユーザの身元を保証し、セキュリティ業務管理手段は身分証明ＩＤによる身元の保証が完了しているユーザに対してのみメッセージの信託サービスなどのセキュリティ業務を提供するので、不正に情報を取得しようとする意図を持つ悪質なユーザを容易に選別および排除することができるという効果が得られる。そして、信託メッセージ秘匿手段はネットワーク経由で送受信されるメッセージの内容を暗号化して、当該メッセージに関わるユーザおよびセキュリティ業務管理手段以外の第三者に知られないようにするので、仮に悪質なユーザにメッセージを取得された場合でも、その盗用などによる損失の発生を未然に防止することができるという効果が得られる。

【００３９】また、証拠情報作成手段は身分証明ＩＤによってセキュリティ業務を利用するユーザのＷＳから送信されてきたメッセージについて生成および送受信が行われた事実を証明するための証拠情報を作成するので、セキュリティ業務を利用するユーザの間で紛争が発生した場合、保管しておいた証拠情報を調べることによって紛争の原因を客観的に突き止めることができるという効果が得られる。そして、改竄防止手段はメッセージの当

事者（例えば、メッセージを作成および送信したユーザと、当該ユーザに対してセキュリティ業務を提供するセキュリティ業務管理手段）以外の第三者に改竄されないようにメッセージのデータ形式を変換するので、メッセージの内容についての信頼性を向上させることができるという効果が得られる。

【００４０】さらに、履歴情報取得手段は稼動中のシステム内で発生した事象を履歴情報として絶えず記録しており、セキュリティ侵害監査手段は記録された履歴情報を常に分析しているので、悪質なユーザによるセキュリティ侵害を迅速に検出して、早期に適切な処置をとることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明のメッセージの信託システムの一構成例を示すブロック図である。

【図２】身分証明ＩＤの発行要求に伴って図１のシステムで行われるデータ通信について概略的に示す図である。

【図３】図２のデータ通信における機密保護のための処理の流れを示すフローチャートである。

【図４】身分証明ＩＤの登録および発行処理に伴って図１のシステムで行われるデータ通信について概略的に示す図である。

【図５】図４のデータ通信における機密保護のための処理の流れを示すフローチャートである。

【図６】メッセージの信託処理に伴って図１のシステムで行われるデータ通信について概略的に示す図である。

【図７】メッセージの信託に際して指定される信託条件の一例を示す図である。

【図８】図６のデータ通信における機密保護のための処理の流れを示すフローチャート（その１）である。

【図９】図６のデータ通信で信託されたメッセージを保管する処理の流れを概略的に示すフローチャートである。

【図１０】図６のデータ通信で作成された証拠情報を確認する処理の流れを示すフローチャートである。

【図１１】図６のデータ通信における機密保護のための処理の流れを示すフローチャート（その２）である。

【図１２】図１中のセキュリティ監査機能を概略的に示すフローチャートである。

【符号の説明】

Ｎ　ネットワークシステム

S_1　身分証明ＩＤ発行サーバ

S_2　身分証明ＩＤ管理サーバ

S_3　セキュリティ業務管理サーバ

WS_{10}，WS_{20}，WS_{30}　ワークステーション

U_1，U_2，U_3　ユーザ

PU_1　ユーザU_1の身分証明ＩＤ

PU_1'　PU_1の引替え証

PK_{U1}，PK_{U3}，PK_{S1}，PK_{S2}，PK_{S3}　公開鍵

SK_{U1}，SK_{U3}，SK_{S1}，SK_{S2}，SK_{S3}　秘密鍵

SSK_1，SSK_2，SSK_3　セション鍵

M，M_1，M_2，M_3，M_1'　メッセージ

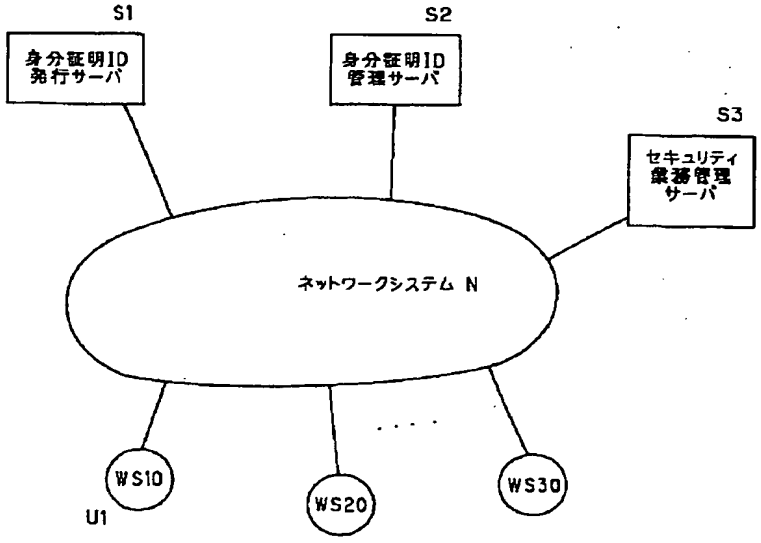
T_0，T_1，T_3，T_4，T_0'　時刻情報

E_1，E_2，E_3，E_1'，E_2'　証拠情報

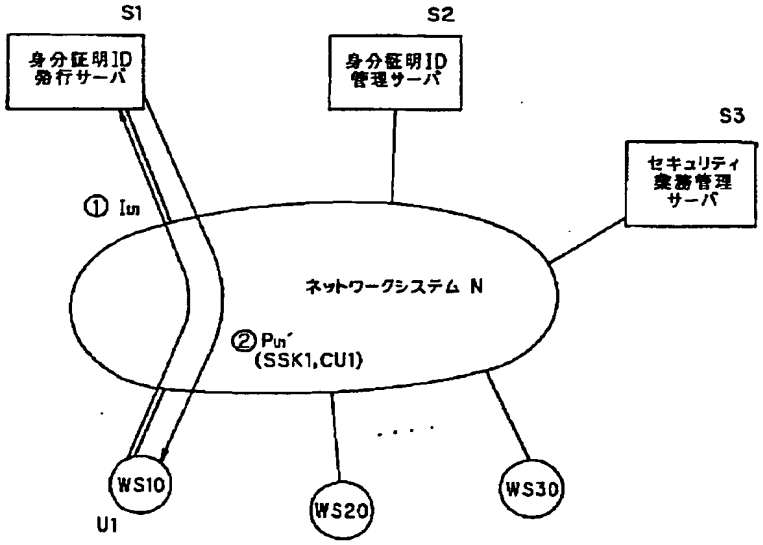
ENC　暗号化関数

DEC　復号化関数

【図１】

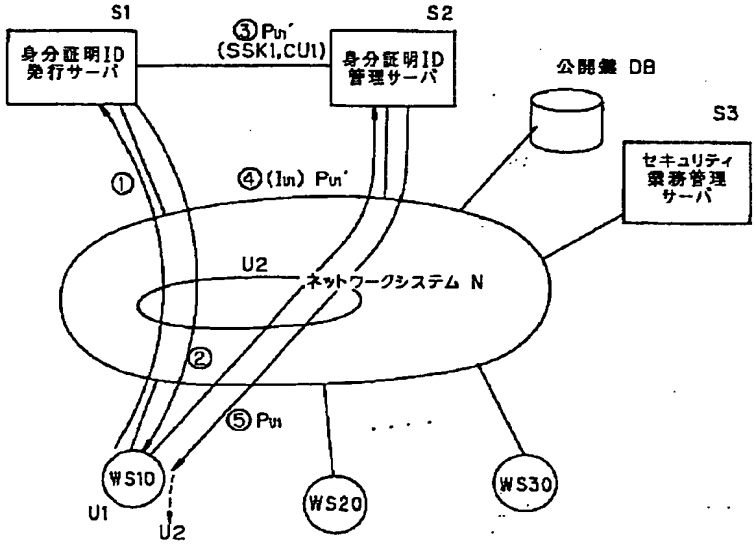


【図２】


S1
身分証明ID
発行サーバ
S2
身分証明ID
管理サーバ
S3
セキュリティ
業務管理
サーバ
① Iun
ネットワークシステム N
② Pun'
(SSK1,CU1)
WS10
U1
WS20
WS30

【図２】

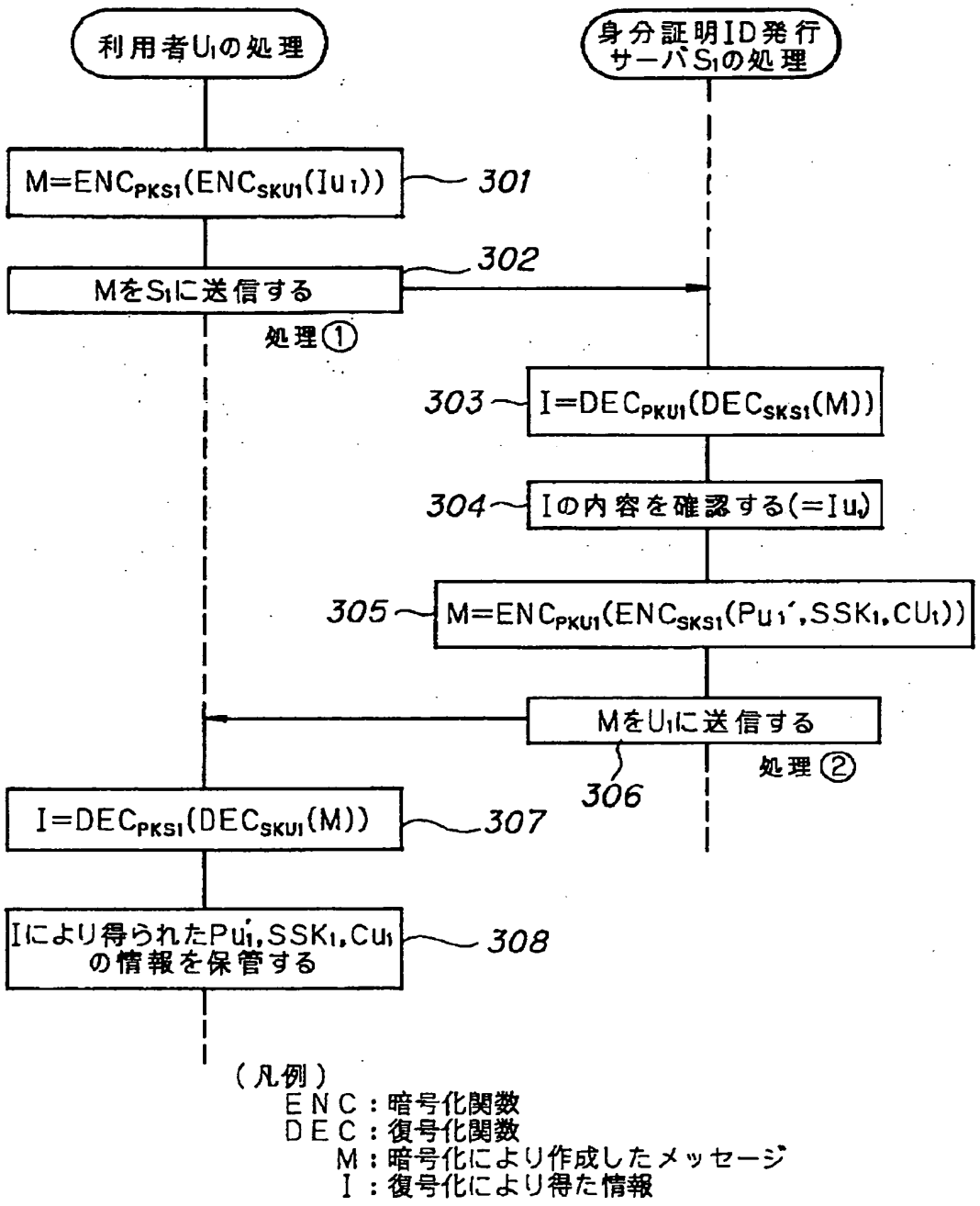
【図４】


S1
身分証明ID
発行サーバ
③ Pun'
(SSK1,CU1)
S2
身分証明ID
管理サーバ
公開鍵 DB
S3
セキュリティ
業務管理
サーバ
①
④ (Iun) Pun'
U2
ネットワークシステム N
②
⑤ Pun
WS10
U1
U2
WS20
WS30

【図４】

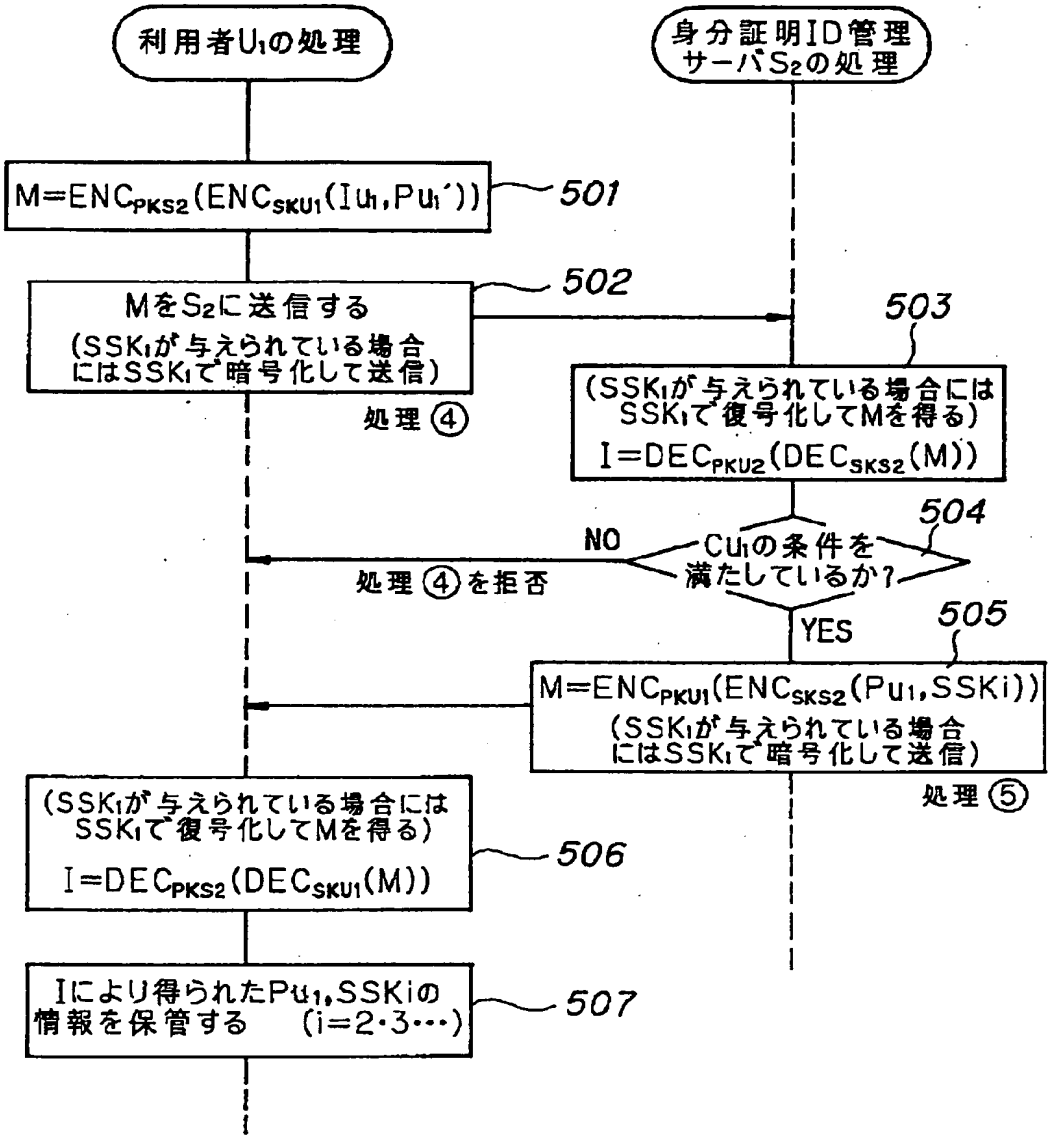
【図３】

【図３】

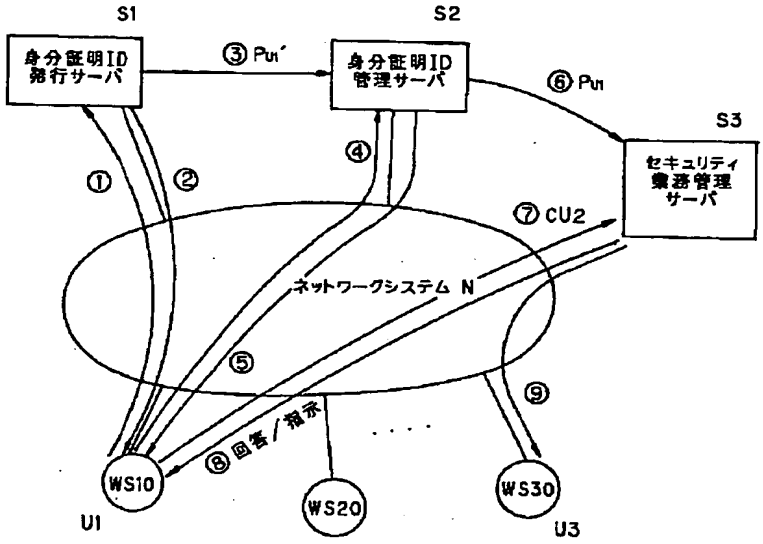

利用者U1の処理
身分証明ID発行サーバS1の処理
M=ENCPKS1(ENCSKU1(Iu1))
301
MをS1に送信する
302
処理①
303
I=DECPKU1(DECSKS1(M))
304
Iの内容を確認する(=Iu1)
305
M=ENCPKU1(ENCSKS1(Pu1',SSK1,CU1))
MをU1に送信する
306
処理②
I=DECPKS1(DECSKU1(M))
307
Iにより得られたPu1',SSK1,CU1の情報を保管する
308
（凡例）
ＥＮＣ：暗号化関数
ＤＥＣ：復号化関数
Ｍ：暗号化により作成したメッセージ
Ｉ：復号化により得た情報

【図5】

【図5】


利用者U1の処理
身分証明ID管理サーバS2の処理
M=ENCPKS2(ENCSKU1(IU1,PU1'))
501
MをS2に送信する
(SSK1が与えられている場合にはSSK1で暗号化して送信)
処理④
502
503
(SSK1が与えられている場合にはSSK1で復号化してMを得る)
I=DECPKU2(DECSKS2(M))
504
CU1の条件を満たしているか?
NO
処理④を拒否
YES
505
M=ENCPKU1(ENCSKS2(PU1,SSKi))
(SSK1が与えられている場合にはSSK1で暗号化して送信)
処理⑤
(SSK1が与えられている場合にはSSK1で復号化してMを得る)
I=DECPKS2(DECSKU1(M))
506
Iにより得られたPU1,SSKiの情報を保管する　(i=2・3…)
507

【図６】



【図７】

【図７】

Cu_2

ドメインマネジャ名称 ＝ S_3
対象メッセージ　　＝ M_1
メッセージ保護レベル　認証レベル　Au=2
アクセス制御レベル　Ac=2
完全性レベル　In=1
機密性レベル　Cn=2
否認不可レベル　Nr=2
オーデットレベル　Ad=1
所有者 ＝ U_1
公開対象 ＝ U_3
公開指定日時 ＝ T_1
破棄指定日時 ＝ T_3

（凡例）

認証レベル　Au
０：認証を行わない
１：ログイン時のみの認証
２：定期的にパスワード入力による認証

アクセス制御レベル　Ac
０：アクセス制御を行わない
１：自システム内のみのアクセス制御
２：他システムも含んだアクセス制御

完全性レベル　In
０：完全性の保護をしない
１：検出コード付加
２：ディジタル署名

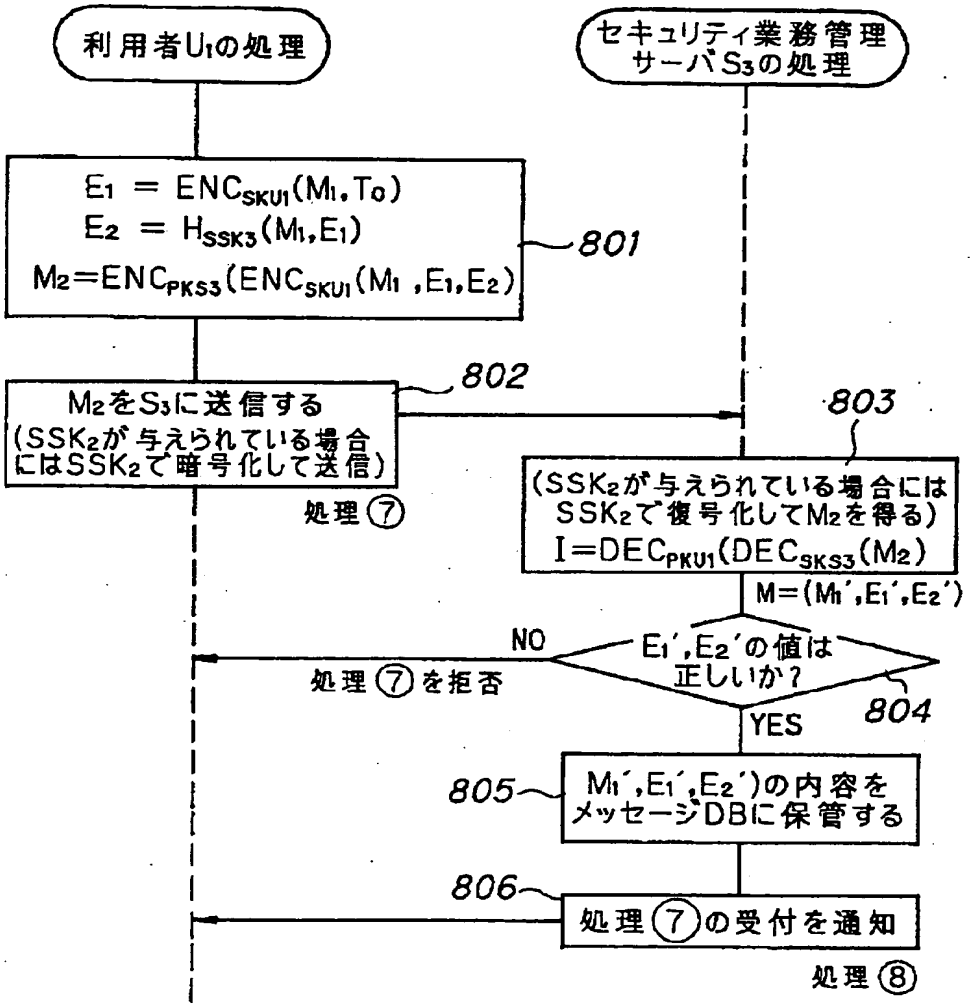
機密性レベル　Cn
０：機密性の保護をしない
１：データの一部の保護
２：データ全体の保護

否認不可レベル
０：否認不可を行わない
１：送信時の証拠作成
２：配送時の証拠作成

オーディットレベル
０：オーディットを行わない
１：アラーム情報の取得
２：セキュリティ報告書の作成

【図８】

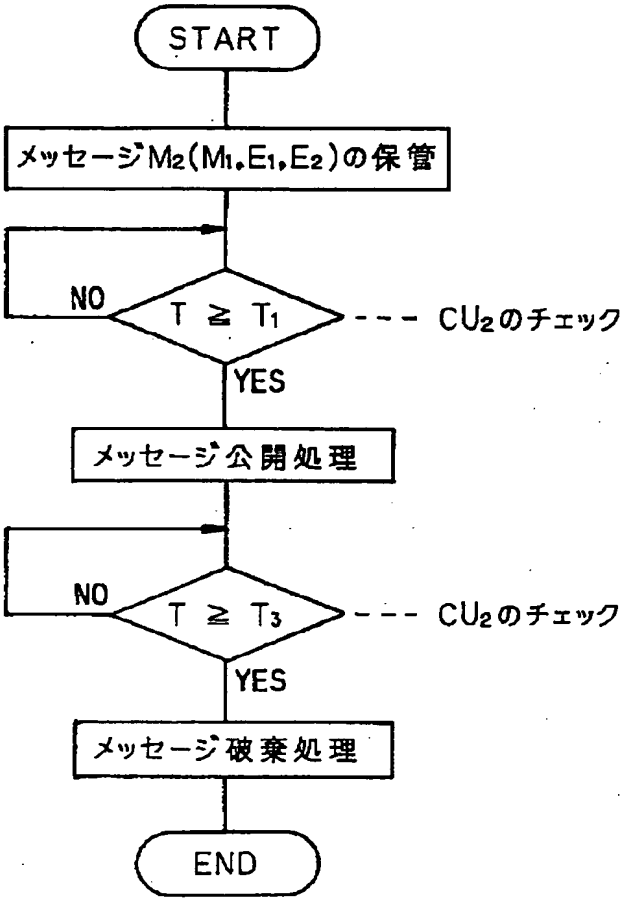
【図８】



（凡例）
H：証拠情報作成用のハッシュ関数
E1,E2：利用者U1が作成した証拠情報
E1',E2'：サーバS3が受信した証拠情報
M1'：サーバS3が受信したメッセージ

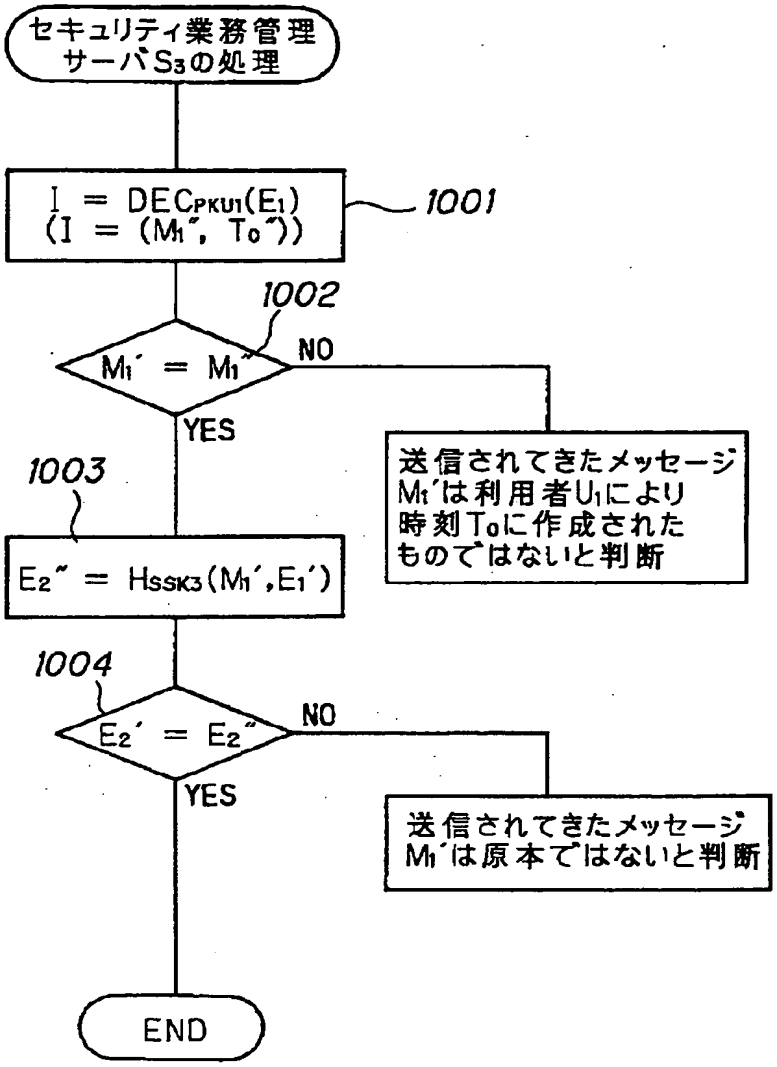
【図9】

【図9】


START
メッセージM2(M1,E1,E2)の保管
NO
T ≧ T1
--- CU2のチェック
YES
メッセージ公開処理
NO
T ≧ T3
--- CU2のチェック
YES
メッセージ破棄処理
END

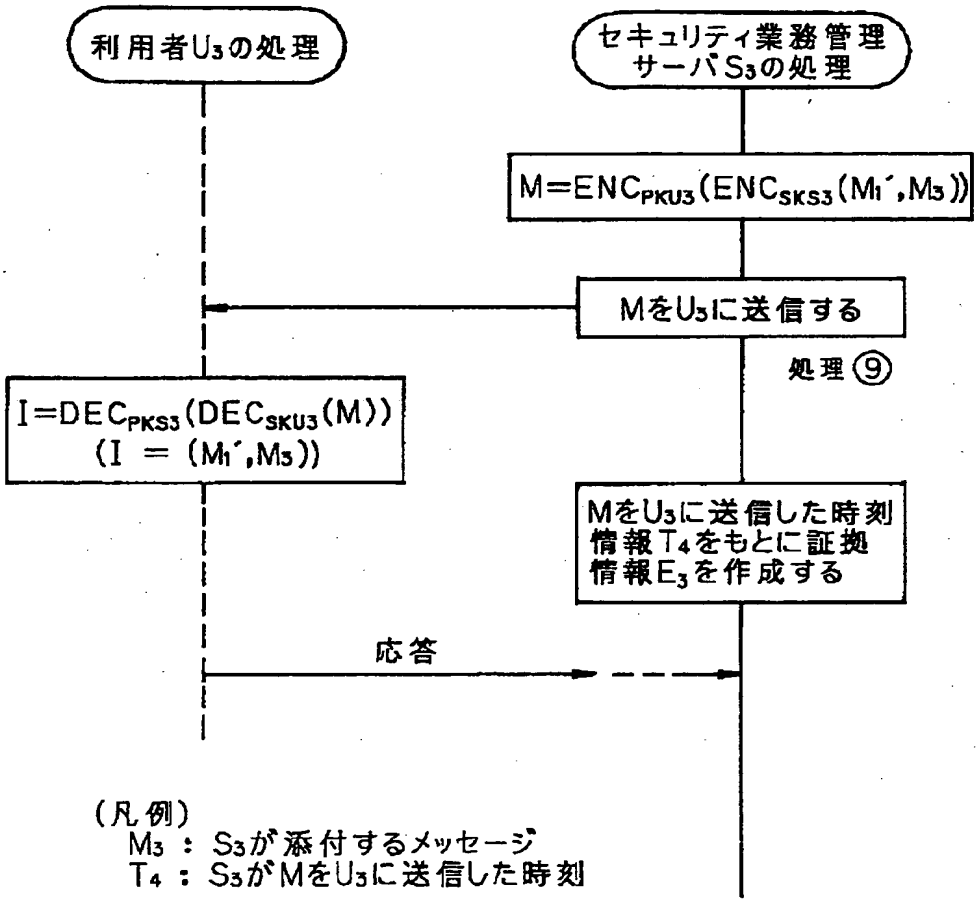
【図10】

【図10】


セキュリティ業務管理
サーバS3の処理
I = DECPKU1(E1)
(I = (M1", T0"))
1001
1002
M1' = M1"
NO
YES
送信されてきたメッセージ
M1'は利用者U1により
時刻T0に作成された
ものではないと判断
1003
E2" = HSSK3(M1',E1')
1004
E2' = E2"
NO
YES
送信されてきたメッセージ
M1'は原本ではないと判断
END

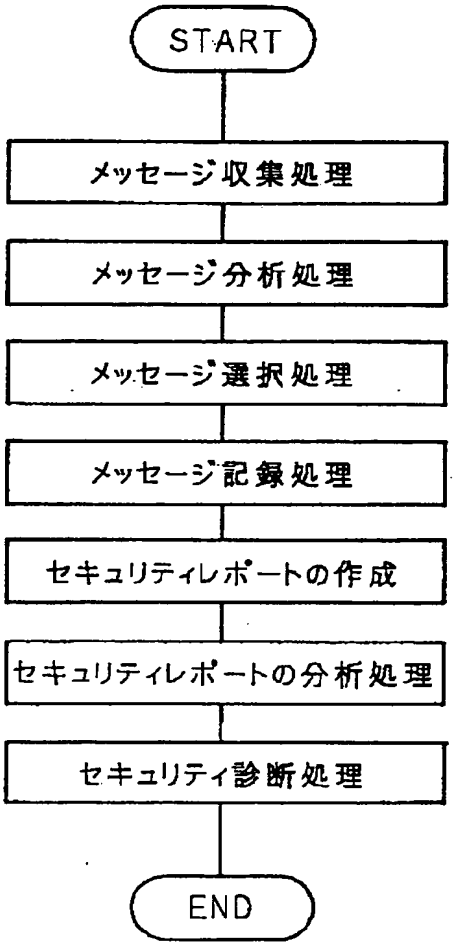
【図１１】

【図11】


利用者U3の処理
セキュリティ業務管理サーバS3の処理
M=ENCPKU3(ENCSKS3(M1´,M3))
MをU3に送信する
処理⑨
I=DECPKS3(DECSKU3(M))
(I = (M1´,M3))
MをU3に送信した時刻情報T4をもとに証拠情報E3を作成する
応答
(凡例)
M3 : S3が添付するメッセージ
T4 : S3がMをU3に送信した時刻

【図12】

【図12】


START
メッセージ収集処理
メッセージ分析処理
メッセージ選択処理
メッセージ記録処理
セキュリティレポートの作成
セキュリティレポートの分析処理
セキュリティ診断処理
END